Journal of Legal Sciences
Pensar
e-ISSN: 2317-2150
Universidade de Fortaleza

10.5020/2317-2150.2025.15238

Diretrizes para a Proteção do Direito Fundamental à Autodeterminação Informativa na Era Digital

Guidelines for the Protection of the Fundamental Right to Informational Self-Determination in the Digital Age

Directrices para la Protección del Derecho Fundamental a la Autodeterminación Informativa en la Era Digital

Ana Maria D´Ávila Lopes *[1], **Rodrigo Martiniano Ayres Lins** *[2]

*Universidade de Fortaleza, Fortaleza, Ceará, Brasil

Editorial

Histórico do Artigo
Recebido: 10/05/2025
Aceito: 22/07/2025

Eixo Temático 3: Direito, Tecnologia e Sociedade em Transformação

Editores-chefes
Katherinne de Macêdo Maciel Mihaliuc
Universidade de Fortaleza, Fortaleza, Ceará, Brasil
katherinne@unifor.br

Sidney Soares Filho
Universidade de Fortaleza, Fortaleza, Ceará, Brasil
sidney@unifor.br

Editor Responsável
Sidney Soares Filho
Universidade de Fortaleza, Fortaleza, Ceará, Brasil
sidney@unifor.br

Autores
Ana Maria D´Ávila Lopes
anadavilalopes@yahoo.com.br
Contribuição: Supervision, Writing – Review & Editing.

Rodrigo Martiniano Ayres Lins
r.martiniano@gmail.com
Contribuição: Conceptualization, Investigation, Writing - Original Draft.

Como citar:
LOPES, Ana Maria D´Ávila; LINS, Rodrigo Martiniano Ayres. Diretrizes para a proteção do direito fundamental à autodeterminação informativa na era digital. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 30, e15238, 2025. DOI: https://doi.org/ 10.5020/2317-2150.2025.15238

Declaração de disponibilidade de dados

A Pensar – Revista de Ciências Jurídicas adota práticas de Ciência Aberta e disponibiliza, junto à presente publicação, a Declaração de Disponibilidade de Dados (Formulário Pensar Data) preenchida e assinada pelos autores, a qual contém informações sobre a natureza do artigo e a eventual existência de dados complementares. O documento pode ser consultado como arquivo suplementar neste site.

Resumo

A consolidação da sociedade digital impôs profundas transformações às dinâmicas sociais, econômicas e jurídicas, gerando riscos inéditos aos direitos fundamentais, sobretudo no que tange à privacidade e à autodeterminação informativa, cuja fragilidade extrapola-se diante da deficiência de uma estrutura normativa capaz de garantir sua proteção. Nesse contexto, o presente artigo busca contribuir a superar essa problemática a partir da formulação de diretrizes direcionadas a aprimorar o arcabouço jurídico nacional, a partir da análise de experiências forâneas. Para tal, a pesquisa adota abordagem qualitativa, valendo-se dos métodos dedutivo e indutivo, com base em revisão bibliográfica e documental da doutrina e jurisprudência nacionais e estrangeiras. A análise parte da compreensão das múltiplas dimensões dos direitos fundamentais na era digital, discute a aplicação do princípio da dignidade da pessoa humana e aprofunda o estudo da autodeterminação informativa enquanto manifestação autônoma do sujeito sobre seus dados pessoais. O trabalho também examina os marcos normativos e jurisprudenciais do Brasil, da Alemanha e da União Europeia. Por fim, propõe diretrizes para a efetivação prática do direito à autodeterminação informativa, tais como a adoção de políticas institucionais baseadas em privacy by design e privacy by default, e a previsão de mecanismos céleres de tutela jurisdicional e administrativa. Conclui-se que a proteção da autodeterminação informativa constitui hoje um imperativo ético e jurídico para a preservação não apenas da dignidade humana, mas também para salvaguardar a confiança no ecossistema digital, inegavelmente inseparável da vida em sociedade na contemporaneidade.

Palavras-chave: direitos fundamentais; autodeterminação informativa; proteção de dados; Tribunal Constitucional Alemão; Tribunal de Justiça da União Europeia.

Abstract

The consolidation of the digital society has imposed profound transformations on social, economic, and legal dynamics, generating unprecedented risks to fundamental rights, especially with regard to privacy and informational self-determination, whose fragility is exacerbated by the deficiency of a normative framework capable of ensuring their protection. In this context, the present article seeks to help overcome this problem by formulating guidelines aimed at enhancing the national legal framework, on the basis of an analysis of foreign experiences. To this end, the research adopts a qualitative approach, employing deductive and inductive methods, grounded in a literature and documentary review of national and foreign legal doctrine and case law. The analysis begins with an understanding of the multiple dimensions of fundamental rights in the digital age, discusses the application of the principle of human dignity, and deepens the study of informational self-determination as an autonomous manifestation of the subject over their personal data. The work also examines the normative and jurisprudential frameworks of Brazil, Germany, and the European Union. Finally, it proposes guidelines for the practical implementation of the right to informational self-determination, such as the adoption of institutional policies based on privacy by design and privacy by default, and the provision of swift mechanisms of judicial and administrative protection. It concludes that the protection of informational self-determination today constitutes an ethical and legal imperative for preserving not only human dignity, but also for safeguarding trust in the digital ecosystem, which is undeniably inseparable from social life in contemporary society.

Keywords: *fundamental rights; informational self-determination; data protection; German Federal Constitutional Court; Court of Justice of the European Union.*

[1] Mestre (1995 - bolsa CAPES) e Doutora (1999 - bolsa CNPq) em Direito Constitucional pela Universidade Federal de Minas Gerais. Pesquisa de pós-doutorado sobre os direitos humanos das minorias e pessoas em situação de vulnerabilidade em: University of British Columbia (Centre for Feminist Legal Studies - 2001), University of Ottawa (Centre de recherche et denseignement sur les droits de la personne - 2001), York University (Osgoode Hall Law School - 2001/ 2002), Yale University (Yale Law School - 2008) e em The University of Auckland (Faculty of Law - 2009/2010) com Bolsa PDE CNPq. Coordenadora da Comissão Qualis-Direito da CAPES (janeiro 2015 - março 2018). Membro da Comissão Qualis-Direito da Capes (2010-2014). Atual Representante da Grande Área das Ciências Sociais no Grupo Assessor Especial da Diretoria de Relações Internacionais (GAE-DIR) da CAPES). Membro Efetivo do Grupo Assessor Especial da Diretoria de Relações Internacionais (GAE-DIR) da CAPES (2017-2019).

[2] Mestre e Doutorando em Direito Constitucional e Teoria Política (UNIFOR - CAPES 6). Especialista em Políticas Públicas para Cidades Inteligentes (USP). Especialista em Direito Eleitoral (PUC/MG), em Direito Processual Civil (Unicap) e em Direito Público (Esmape). Atualmente é Procurador-Geral da Assembleia Legislativa do Estado do Ceará e Professor de Cursos de Pós-Graduação em Direito. Membro-fundador da Academia Brasileira de Direito Eleitoral e Político (ABRADEP).

© 2025 Revista Pensar – Revista de Ciências Jurídicas. Este é um artigo publicado em acesso aberto sob a licença Creative Commons Atribuição (CC-BY 4.0 Internacional).

Resumen

La consolidación de la sociedad digital impuso profundas transformaciones a las dinámicas sociales, económicas y jurídicas, generando riesgos inéditos para los derechos fundamentales, especialmente en lo que atañe a la privacidad y a la autodeterminación informativa, cuya fragilidad se ve acrecentada ante la insuficiencia de una estructura normativa capaz de garantizar su protección. En este contexto, el presente artículo busca contribuir a superar esta problemática mediante la formulación de directrices orientadas a perfeccionar el armazón jurídico nacional, a partir del análisis de experiencias foráneas. Para ello, la investigación adopta un enfoque cualitativo, valiéndose de los métodos deductivo e inductivo, con base en una revisión bibliográfica y documental de la doctrina y la jurisprudencia nacionales y extranjeras. El análisis parte de la comprensión de las múltiples dimensiones de los derechos fundamentales en la era digital, discute la aplicación del principio de la dignidad de la persona humana y profundiza el estudio de la autodeterminación informativa como manifestación autónoma del sujeto sobre sus datos personales. El trabajo también examina los marcos normativos y jurisprudenciales de Brasil, Alemania y la Unión Europea. Por último, propone directrices para la efectivación práctica del derecho a la autodeterminación informativa, tales como la adopción de políticas institucionales basadas en privacy by design y privacy by default, y la previsión de mecanismos expeditos de tutela jurisdiccional y administrativa. Se concluye que la protección de la autodeterminación informativa constituye hoy un imperativo ético y jurídico para la preservación no solo de la dignidad humana, sino también para salvaguardar la confianza en el ecosistema digital, innegablemente inseparable de la vida en sociedad en la contemporaneidad.

Palabras clave*: derechos fundamentales; autodeterminación informativa; protección de datos; Tribunal Constitucional Federal de Alemania; Tribunal de Justicia de la Unión Europea.*

1 Introdução

A revolução tecnológica e a consolidação da sociedade da informação transformaram radicalmente o modo como os indivíduos interagem, produzem conhecimento e exercem direitos. No centro dessas transformações, encontra-se a crescente centralidade dos dados pessoais, cujo tratamento massivo, por entes públicos e privados, impõe novos desafios ao direito constitucional contemporâneo.

A transição para uma sociedade conectada afeta tanto as nações mais industrializadas quanto as economias em desenvolvimento, configurando um paradigma global pautado nas tecnologias da informação (Castells, 2000). As relações sociais passaram a ser mediadas por redes digitais e sistemas de vigilância capazes de reorganizar estruturas econômicas e políticas, redefinindo os contornos da vida privada e da autonomia individual.

Nesse cenário, a coleta, o armazenamento e a monetização de dados tornaram-se práticas generalizadas, especialmente por grandes plataformas digitais. Embora esses fluxos informacionais permitam inovação e personalização de serviços, também geram assimetrias de poder, riscos à privacidade, discriminação algorítmica e manipulação comportamental. Tais vulnerabilidades evidenciam a urgência de uma resposta jurídica mais adequada.

Diante dessa reconfiguração das estruturas sociais e jurídicas impulsionadas pelas tecnologias digitais, torna-se indispensável repensar a configuração dos direitos fundamentais à luz das dinâmicas próprias da sociedade informacional. A autodeterminação informativa, concebida como expressão da dignidade humana e da autonomia individual, emerge como um dos direitos mais desafiados e, ao mesmo tempo, mais relevantes deste novo tempo.

Nesse contexto, o presente artigo tem por objetivo formular diretrizes para o aprimoramento do arcabouço jurídico do direito fundamental à autodeterminação informativa, diante de uma estrutura normativa ainda deficiente. Desse modo, busca-se analisar seu surgimento como resposta constitucional às assimetrias e riscos impostos pela lógica digital contemporânea, que colocam em risco o direitos dos indivíduos de decidir quais dados pessoais podem ser coletados e como podem ser usados.

A pesquisa desenvolve-se por meio de análise bibliográfica e documental, de caráter qualitativo e narrativo, valendo-se dos métodos dedutivo e indutivo. A abordagem mobiliza doutrina nacional e estrangeira, bem como jurisprudência do Supremo Tribunal Federal, do Tribunal Constitucional Federal Alemão e do Tribunal de Justiça da União Europeia, com o intuito de oferecer uma leitura crítica da autodeterminação informativa na sociedade digital.

Em uma era de informação e interconexão, garantir esse direito representa um imperativo ético indispensável para a salvaguarda da dignidade humana, sob pena de manter-se como um direito declaratório frente a estruturas privadas de poder informacional desproporcionais e assimétricas.

2 Os direitos fundamentais na era digital

Os direitos fundamentais constituem um dos mais importantes pilares sobre os quais se constrói o Estado Democrático de Direito. Eles são direitos cuja titularidade corresponde a todos os seres humanos, independentemente de nacionalidade, sexo, origem étnica ou racial, religião, linguagem, ou qualquer outra condição. “A previsão dos direitos humanos fundamentais direciona-se basicamente para a proteção à dignidade humana em seu sentido mais amplo” (Moraes, 1998, p. 22).

Estes direitos abrangem diversas dimensões, incluindo, mas não se limitando a direitos civis, políticos, econômicos, sociais e culturais, refletindo a complexidade e a interdependência dos aspectos que compõem a vida em sociedade. A positivação desses direitos, de natureza humana, "indica, por exemplo, se um Estado pode ou não ser reconhecido como democrático ou se assume ares de barbárie" (Souza; Mezzaroba, 2012, p. 175).

Na dimensão civil, os direitos fundamentais focam na proteção da liberdade e da integridade pessoal. Isso inclui o direito à vida, à liberdade, à igualdade, *à privacidade* e à propriedade. Estes direitos são essenciais para o desenvolvimento do indivíduo, permitindo-lhe expressar-se livremente, buscar e receber informações. Ademais, "tendem a limitar o poder do Estado e a reservar para o indivíduo, ou para grupos particulares, uma esfera de liberdade e relação ao Estado" (Bobbio, 2004, p. 23).

Na esfera política, os direitos fundamentais garantem a participação dos cidadãos na vida política e nos processos decisórios que afetam suas vidas. Isso envolve o direito de votar e ser votado, bem como de ocupar cargos públicos. Trata-se de direitos de "participação cada vez mais ampla, generalizada e frequente dos membros de uma comunidade no poder político" (Bobbio, 2004, p. 23).

Do ponto de vista econômico, os direitos fundamentais visam assegurar a livre iniciativa, de modo a proteger e promover o desenvolvimento econômico individual, que repercutirá no próprio desenvolvimento do Estado.

No âmbito social, os direitos fundamentais permitem exigir do Estado a implementação de ações direcionadas à satisfação das condições mínimas para uma vida digna, como a proteção ao trabalho, incluindo, por exemplo, uma remuneração justa e satisfatória, além de direitos capitais para o bem-estar econômico dos indivíduos e suas famílias como o direito à educação, à saúde, à assistência aos desamparados, à seguridade social, e a um padrão de vida adequado. Eles são fundamentais para garantir que todos tenham acesso aos recursos básicos necessários para viver com dignidade e participar plenamente na sociedade.

Por fim, na dimensão cultural, os direitos fundamentais reconhecem a diversidade cultural, de modo a proteger o direito de cada pessoa de participar da vida cultural da comunidade à que pertencem, desfrutando tradições, das artes e outras manifestações que fazem parte da sua própria identidade.

Em suma, os direitos fundamentais são a expressão mais profunda da proteção da dignidade humana, servindo como normas jurídicas que viabilizam a convivência pacífica e harmônica de todos os seus membros da sociedade.

Na era digital, o exercício, a proteção e a promoção dos direitos fundamentais assumem novas dimensões, desafiando as sociedades a repensar e adaptar os princípios tradicionais aos ambientes virtuais. Trata-se de uma nova era, que amplia o escopo de aplicação dos direitos fundamentais e destaca novas vulnerabilidades e desafios que surgem a partir da sua confluência com a tecnologia.

E, "no ambiente digital, os atores privados surgem ao lado dos Estados-Nação como potenciais infratores dos direitos fundamentais" (Celeste, 2021, p. 86). Assim, a proteção e a promoção dos direitos fundamentais exigem uma constante atualização interpretativa, a fim de assegurar sua eficácia diante das novas vulnerabilidades e assimetrias de poder que emergem no espaço virtual.

Na dimensão civil, a proteção do direito à privacidade e à proteção de dados pessoais se torna central, dada a capacidade, sem precedentes, de coletar, armazenar e processar informações pessoais online. O respeito pela privacidade e a autonomia sobre os próprios dados são essenciais para garantir a liberdade individual na era digital. Isso implica em desafios relacionados à vigilância em massa, ao rastreamento online e ao uso indevido de dados por entidades privadas e governamentais.

No âmbito político, a internet possibilita uma difusão de ideias sem precedentes, promovendo a participação cidadã e a democracia. No entanto, também expõe riscos relacionados à censura digital, à desinformação e aos discursos de ódio online. Garantir que o ambiente digital seja um espaço para o discurso democrático, respeitando a diversidade de opiniões e protegendo contra abusos, torna-se um imperativo.

Economicamente, a era digital transformou o mercado de trabalho e a economia global, criando novas formas de emprego e desafios relacionados à segurança no emprego, à proteção de direitos trabalhistas e à desigualdade econômica. A capacidade de trabalhar remotamente e a *gig economy são exemplos de como os direitos econômicos precisam ser adaptados e protegidos no contexto digital.*

Socialmente, a inclusão digital *é decisiva* para garantir que todos tenham igual acesso às políticas públicas de bem-estar social, garantindo a superação das desigualdades econômicas. Contudo, a necessidade de estar conectado digitalmente às plataformas públicas traz o risco da perda da privacidade.

Culturalmente, o contexto digital oferece novas plataformas que promovem o conhecimento e intercâmbio entre culturas. No entanto, também levanta questões sobre direitos autorais, apropriação cultural e a preservação da diversidade cultural na era digital.

Assim, a interseção dos direitos fundamentais com o contexto digital demanda um reequilíbrio entre liberdade e segurança, privacidade e transparência, inclusão e diversidade. Requer uma reflexão contínua sobre como os direitos fundamentais podem ser efetivamente exercidos e protegidos no ambiente digital, assegurando que a tecnologia sirva ao bem-estar humano e promova uma sociedade mais justa e inclusiva. O desafio reside em desenvolver políticas, regulamentações e tecnologias que respeitem e fortaleçam os direitos fundamentais, garantindo que os avanços digitais contribuam positivamente para a humanidade.

A era digital, caracterizada pela revolução tecnológica e a ubiquidade das tecnologias de informação e comunicação, trouxe consigo transformações sem precedentes em praticamente todos os aspectos da vida humana. Essas mudanças têm impactado profundamente a maneira como compreendemos e exercemos os direitos fundamentais, tais como a liberdade de expressão, o direito à privacidade, a liberdade de imprensa, o acesso à informação e a proteção contra discriminação.

A expansão das redes digitais e o aumento do poder de processamento e armazenamento de dados têm possibilitado uma maior conexão entre as pessoas e o acesso a uma quantidade infinita de informações. No entanto, essa mesma expansão trouxe desafios significativos para a proteção e a promoção dos direitos fundamentais. Questões como a vigilância em massa, a coleta e o uso indevidos de dados pessoais, a disseminação de desinformação, os discursos de ódio online e a censura digital são apenas alguns dos problemas emergentes que necessitam de atenção urgente.

Alcançamos a constituição de uma identidade digital, mas ainda não dispomos de um espaço seguro que possa ser considerado sua morada legítima. Tampouco existem mecanismos institucionais efetivos de proteção coletiva de dados ou um espaço cibernético que garanta pertencimento e autonomia. Nem mesmo gigantes tecnológicos como Google e Meta — e menos ainda o Estado e suas agências de segurança e informação — asseguram esse abrigo. Importa reconhecer, contudo, que esse “eu digital” não corresponde a uma extensão ontológica do sujeito, mas a uma construção relacional, moldada por sistemas de vigilância contínua, registros civis, identificação unívoca de cidadãos, dispositivos conectados, armazenamento em nuvem, drones, dados biométricos, bases de comunicação e perfilamento algorítmico. Nesse contexto, garantias como a privacidade, o direito ao esquecimento ou a possibilidade de tornar-se invisível no ambiente digital emergem como expressões de novos direitos fundamentais. É nesse horizonte que se pode falar em uma noção de fundamentalidade digital (Canotilho, 2019).

Nesse cenário, ganha relevo o Constitucionalismo Digital, concebido como o esforço teórico e normativo de reconhecer, afirmar e proteger os direitos fundamentais no ciberespaço, diante da assimetria de poder informacional entre usuários, corporações e Estados. Além da tutela de direitos, o Constitucionalismo Digital busca restaurar o equilíbrio entre os diversos atores da esfera digital, enfrentando os riscos impostos pelo capitalismo de vigilância, pela extração massiva e não consentida de dados — o chamado superávit comportamental — e pelas práticas globais de colonialismo informacional que comprometem a soberania individual e coletiva sobre os dados (Cantarini, 2023).

Torna-se imperativo, pois, que as sociedades reflitam sobre como os direitos fundamentais podem ser preservados e fortalecidos na era digital, considerando que “o reconhecimento e a proteção dos direitos do homem são a base das constituições democráticas” (Bobbio, 2004, p. 223). Isso implica em adaptar os marcos regulatórios existentes e desenvolver novas abordagens que levem em consideração as particularidades do ambiente digital. O objetivo é garantir que a tecnologia atue como uma facilitadora da liberdade e da democracia, e não como uma ferramenta para sua erosão.

Além disso, a era digital coloca em destaque a necessidade de promover a inclusão e garantir que todos tenham acesso às tecnologias de informação e comunicação, como dito. Afinal, a capacidade de acessar e usar a informação é fundamental para o exercício dos direitos humanos e a participação efetiva na sociedade contemporânea.

Portanto, enquanto navegamos por esta nova era, é fundamental que governos, empresas, organizações da sociedade civil e indivíduos trabalhem juntos para assegurar que a tecnologia sirva ao bem comum, promovendo os direitos fundamentais e contribuindo para uma sociedade mais justa, inclusiva e democrática.

3 O direto fundamental à autodeterminação informativa nas plataformas digitais

No seio da Constituição Federal de 1988 (Brasil, 1988), o Brasil consagrou uma série de direitos e garantias fundamentais, reflexo das aspirações democráticas e dos anseios de uma sociedade em busca de justiça, liberdade e igualdade. É tal a importância desses direitos e garantais, que o constituinte não se limitou a listá-los expressamente,

mas estabeleceu uma cláusula de abertura de modo a incluir aqueles que, por acaso, tivessem sido omitidos ou que, pelo desenvolvimento natural da sociedade, fosse necessário adicioná-los à ordem constitucional. Essa cláusula encontra-se acolhida no artigo 5º, §2º, no qual se estabelece que os direitos e garantias fundamentais previstos na Constituição não excluem outros derivados dos princípios ou do regime por ela adotados, ou aqueles constantes dos tratados internacionais dos quais o Brasil faça parte (Brasil, 1988). Esta norma reflete a intenção do constituinte de considerar a existência de direitos e garantias fundamentais fora do texto constitucional, ou seja, de normas materialmente constitucionais que, pela sua qualidade de parâmetros axiológicos, devem ser considerados parte da ordem constitucional. Nessa linha pronuncia-se Piovesan (1998, p. 52) "[...] advém de interpretação sistemática e teleológica do texto, especialmente em face da força expansiva dos valores da dignidade humana e dos direitos fundamentais, como parâmetros axiológicos a orientar a compreensão do fenômeno constitucional".

Afinal, "os direitos fundamentais não se esgotam naqueles direitos reconhecidos no momento constituinte originário, mas estão submetidos a um permanente processo de expansão" (Pardo, 2015, p. 12).

Nesse contexto, emergiu, na doutrina, a noção de que a autodeterminação informativa, embora não prevista expressamente como um direito fundamental na Lei Maior, se encontra implicitamente resguardada como tal pelo texto constitucional, considerando derivar do princípio fundamental da dignidade da pessoa humana.

A dignidade da pessoa humana, consolidada no artigo 1º, inciso III da Constituição (Brasil, 1988), é o pilar basilar do ordenamento jurídico brasileiro. Este princípio relaciona-se diretamente com a autonomia, o livre desenvolvimento e o reconhecimento do valor intrínseco de cada ser humano. No ambiente digital contemporâneo, onde as informações e os dados pessoais se tornam extensões da personalidade do indivíduo, garantir sua integridade e controle torna-se imperativo para a preservação dessa dignidade.

No ambiente digital atual, as empresas – e não apenas o Estado – desempenham um papel central na coleta, processamento e armazenamento de dados pessoais. Empresas tecnológicas globais, redes sociais e plataformas online têm acesso a uma quantidade sem precedentes de dados sobre os indivíduos, muitas vezes mais do que o próprio Estado. E a verdade é que o "controle sobre os dados pessoais por parte dos titulares é uma ilusão diante da economia digital capitalizada pelas big techs" (Pessoa; Limberger; Witschoreck, 2024, p. 11).

Diante desse contexto, torna-se cada vez mais manifesto que o controle sobre os próprios dados pessoais é parte inseparável da liberdade individual e da autonomia da vontade. Como aponta Zuboff (2019), a lógica do capitalismo de vigilância opera por meio da extração unilateral de dados comportamentais, transformando cada aspecto da vida cotidiana em matéria-prima para modelos preditivos. Essa assimetria informacional, muitas vezes invisível e incontornável, compromete a autodeterminação dos indivíduos, ao submeter suas escolhas a estruturas algorítmicas sem transparência e interesses comerciais que escapam ao seu controle. Proteger os dados, portanto, é proteger a própria possibilidade de agir livremente em uma sociedade digitalizada.

Nesse sentido, o direito à autodeterminação informativa consiste no poder do indivíduo de decidir quais dados pessoais podem ser coletados e como podem ser usados. É o exercício de sua autonomia sobre suas informações, permitindo que ele tenha controle sobre sua identidade digital e narrativa pessoal. Deve-se ter o "direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular" (Rodotà, 2008, p. 15).

A autodeterminação informativa representa o "direito a controlar o uso que os outros fazem das informações que digam respeito à esfera privada do indivíduo" (Doneda, 2000, p. 120). "Um cadastro pode armazenar um número quase ilimitado de informação. Assim, o indivíduo que confia seus dados deve contar com a tutela jurídica para que estes sejam utilizados corretamente, seja em entidades públicas ou privadas" (Limberger, 2009, p. 58). Ao conceber a esfera íntima como um agrupamento de atitudes, comportamentos, preferências, opiniões e ações que o sujeito deseja preservar sob seu domínio exclusivo, a proteção [à privacidade] deve se fundamentar no "direito de autodeterminação informativa" (Doneda, 2020, p. 129).

A facilidade de acesso aos dados pessoais pelas plataformas digitais, além da velocidade desse acesso, da transmissão e o seu cruzamento, "potencializa as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social" (Sarlet, 2020, p. 181). Isso significa que, antes de qualquer coleta ou uso de dados e informações, o indivíduo deve ter conhecimento claro e dar seu consentimento informado. O manejo de dados pessoais, portanto, se não regido por critérios claros e limites estritos, pode violar essa esfera íntima do indivíduo.

A ideia por trás dessa autodeterminação é que o indivíduo seja o principal agente na decisão sobre o destino e uso de suas informações. Não se trata apenas de ser informado, mas de ter a capacidade e o poder de influenciar ativamente as decisões sobre seus dados.

O direito à autodeterminação informativa não deve ser confundido com o direito à privacidade e com o direito de proteção de dados, pois, embora estejam inter-relacionados e muitas vezes se sobreponham, eles têm nuances e focos distintos. É essencial reconhecer essas diferenças para garantir sua proteção eficaz no mundo digital.

Assim, o direito à privacidade, que se conecta, mas é diverso do direito à autodeterminação informativa, é um conceito mais amplo e antigo, que protege o indivíduo de interferências indesejadas em sua vida privada. Enquanto a autodeterminação informativa está centrada especificamente na gestão de dados pessoais, a privacidade engloba uma série de aspectos mais amplos da intimidade individual como a proteção das suas comunicações telefônicas e a inviolabilidade do seu domicílio.

Embora ambos os conceitos estejam interligados, é possível ter uma invasão de privacidade sem necessariamente afetar a autodeterminação informativa e vice-versa. Por exemplo, uma escuta telefônica sem consentimento viola a privacidade, mas se os dados coletados não forem usados ou compartilhados, a autodeterminação informativa pode não ser comprometida.

O direito à proteção de dados, recentemente incorporado à Constituição Federal por meio da Emenda Constitucional nº 115, de 10 de fevereiro de 2022 (Brasil, 2022), por sua vez, refere-se a garantias legais e práticas que asseguram que os dados pessoais sejam coletados, processados, armazenados e compartilhados de forma segura e em conformidade com as normas estabelecidas. Embora esteja intrinsecamente relacionada à autodeterminação informativa, a proteção de dados tem um foco mais técnico e procedural, enquanto a autodeterminação informativa tem uma abordagem centrada na autonomia do sujeito titular desses dados. Assim, por exemplo, é possível que uma empresa siga todas as normas de proteção de dados (como criptografia e políticas de acesso), mas ainda assim viole o princípio da autodeterminação informativa ao não obter consentimento adequado ou ao usar dados de uma maneira que o indivíduo não tenha de fato concordado.

O preceito de autodeterminação informativa obteve reconhecimento no ano de 1983 pelo Tribunal Constitucional Federal Alemão (Bundesverfassungsgericht), ao proferir uma decisão declarando a inconstitucionalidade da “Lei do Censo”. A norma prescrevia que os cidadãos alemães deveriam providenciar um conjunto abrangente de dados pessoais com a finalidade de permitir ao Estado conduzir uma análise estatística sobre a distribuição demográfica, tanto em termos espaciais quanto geográficos, além de permitir que esses dados fossem cruzados com outros tipos de registros públicos (Bioni, 2021).

Essa decisão representa, conforme observa Laura Schertel Ferreira Mendes (2020), um momento de virada na proteção da personalidade, ao reconhecer que o Estado não pode coletar dados pessoais de forma coercitiva sem respeitar a esfera íntima do indivíduo. Tal julgamento firmou a compreensão de que a autodeterminação informativa é condição indispensável ao livre desenvolvimento da personalidade, inserindo a proteção de dados no núcleo dos direitos fundamentais.

Em 2019, o referido Tribunal voltou a reconhecer que o direito a autodeterminação informativa não se limita às relações com o Estado, estendendo-se também às práticas de exploração comercial de dados por grandes empresas de tecnologia, conferindo mais densidade à aplicação horizontal dos direitos fundamentais no ambiente digital. Ao enfrentar os efeitos da chamada *datafication*, marcada pela onipresença de dados e pela concentração de poder informacional nas mãos de poucas plataformas, o Tribunal reafirmou a necessidade de que os indivíduos tenham controle real sobre o tratamento de suas informações pessoais, não apenas como expressão formal de consentimento, mas como manifestação concreta de autonomia informacional em face de agentes privados (Gstrein; Beaulieu, 2022).

Mais recentemente, no julgamento do processo 1 BvR 1160/19, de 1º de outubro de 2024 (Alemanha, 2024), o Bundesverfassungsgericht voltou a se debruçar sobre os limites constitucionais da atuação estatal em matéria de tratamento de dados pessoais, reafirmando os contornos normativos do direito à autodeterminação informativa. A Corte declarou a inconstitucionalidade de dispositivos da Lei do Escritório Federal de Investigação Criminal (BKA-Gesetz) que autorizavam, de forma desproporcional, a vigilância invasiva de pessoas meramente vinculadas a suspeitos — as chamadas “pessoas de contato” — bem como a manutenção preventiva de dados em plataformas policiais federais, sem critérios claros de vinculação com a finalidade da medida.

Na decisão, o Tribunal reiterou que a coleta e o armazenamento de dados pessoais devem respeitar limites objetivos de necessidade, adequação e temporalidade. O simples potencial de utilidade futura não legitima, por si

só, a conservação das informações, sendo indispensável a previsão legal de prazos de retenção e de critérios de atualização, além da obrigação de exclusão dos dados quando atingido o fim que justificou sua coleta. A decisão evidencia, assim, a maturidade da doutrina constitucional alemã na defesa da esfera privada em tempos de vigilância digital e reforça o papel da autodeterminação informativa como pilar da proteção da personalidade diante do avanço das tecnologias de monitoramento estatal e da interoperabilidade entre bases de dados.

No Brasil, o Supremo Tribunal Federal reconheceu a autodeterminação informativa como um direito fundamental no julgamento da Medida Cautelar da Ação Direta de Inconstitucionalidade n° 6387-DF (MC-ADI 6387-DF), em 7 de maio de 2020 (Brasil, 2020), na qual se debateu sobre a constitucionalidade da Medida Provisória n° 954, de 17 de abril de 2020, que determinava a transferência de dados de usuários de serviços de telefonia ao Instituto Brasileiro de Geografia e Estatística (IBGE), no contexto da pandemia da covid-19 (Brasil, 2022). A Ministra Rosa Weber entendeu, *ad referendum* da Corte, que tal transferência, sem o devido consentimento dos titulares, violaria, dentre outros direitos, a autodeterminação informativa:

> A afirmação da autonomia do direito fundamental à proteção de dados pessoais – há de se dizer – não se faz tributária de mero encantamento teórico, mas antes da necessidade inafastável de afirmação de direitos fundamentais nas sociedades democráticas contemporâneas. Considerando que os espaços digitais são controlados por agentes econômicos dotados de alta capacidade de coleta, armazenamento e processamento de dados pessoais, a intensificação do fluxo comunicacional na internet aumenta as possibilidades de violação de direitos de personalidade e de privacidade (Brasil, 2020, p. 14).

Verifica-se, portanto, a preocupação do Supremo Tribunal Federal, guardião da Constituição, de conferir proteção constitucional à autodeterminação informativa no contexto da era digital, controlada por agentes econômicos com grande poder para colocar em risco os direitos fundamentais.

Apesar de anos antes, a Lei nº 13.709, Lei Geral de Proteção de Dados (LGPD), de 14 de agosto de 2018, ter previsto expressamente a proteção à autodeterminação informativa no art. 2°, II (Brasil, 2018), era necessário o reconhecimento formal da sua qualidade de direito fundamental, o que veio com essa decisão do Supremo Tribunal Federal, que tem também o mérito de ter feito referência expressa aos riscos que esse direito enfrenta no contexto da era digital. Preencheu, dessa forma, uma grave lacuna protetiva ao confirmar a eficácia horizontal do direito fundamental à autodeterminação informativa.

No ordenamento jurídico europeu, o Regulamento Geral sobre a Proteção de Dados (GDPR - Regulamento UE 2016/679) (União Europeia, 2016) consolida a proteção do direito à autodeterminação informativa ao estabelecer obrigações diretamente aplicáveis ao Estado e às entidades privadas que atuam como controladoras ou processadoras de dados pessoais. Essa vinculação expressa decorre do artigo 1.2, que define como objetivo do regulamento a proteção das pessoas singulares independentemente do setor (público ou privado), além dos princípios gerais do tratamento de dados (art. 5).

Uma das decisões paradigmáticas do Tribunal de Justiça da União Europeia (TJUE) foi no caso Google Spain, no qual estabeleceu que ferramentas de busca, como operadores privados, estão sujeitos às obrigações do regulamento, reconhecendo o chamado “direito ao esquecimento” (União Europeia, 2016, art. 17) como um direito fundamental aplicável mesmo nas relações entre particulares (TJUE, 2014).

Posteriormente, em Schrems II, o Tribunal ampliou esse entendimento ao declarar inválido o *Privacy Shield* — acordo de transferência de dados entre a UE e os EUA — por considerar que as empresas estadunidenses não garantiam um nível de proteção ‘essencialmente equivalente’ ao da UE, conforme exigido pelo artigo 45.º do GDPR (TJUE, 2020). Essa decisão reforçou a extraterritorialidade do regulamento e a responsabilidade direta de controladores de dados, inclusive em operações transfronteiriças, submetendo-as ao crivo dos direitos fundamentais europeus (União Europeia, 2012, art. 7, art. 8).

Ademais, o TJUE destacou que as empresas privadas devem realizar avaliações independentes sobre a legalidade de transferências internacionais, que devem considerar a legislação local do país de destino e o acesso de autoridades públicas a esses dados (TJUE, 2020).

As empresas que operam no ambiente digital têm o potencial de afetar profundamente a autodeterminação informativa e, portanto, devem ser responsabilizadas quando negligenciam ou violam esse direito.

É válido ressaltar que o reconhecimento do direito à autodeterminação informativa não significa que as empresas não possam tratar dados pessoais. Significa, sim, que esse tratamento deve ser feito de forma

transparente, responsável e alinhada aos princípios constitucionais e legais, garantindo aos indivíduos o controle e a autodeterminação sobre suas próprias informações.

A natureza dos serviços oferecidos pelas plataformas digitais, que se fundamenta no uso extensivo de dados, torna imperativo que atuem sob um padrão rigoroso de proteção. Nesse sentido, as entidades não podem se eximir de suas responsabilidades, apoiando-se no argumento de que são meramente entes privados. A sua atuação no mundo digital coloca-as em uma posição que pode ser comparada a verdadeiras entidades públicas no que tange à magnitude de suas responsabilidades perante os direitos fundamentais.

O uso indiscriminado de dados ou a falta de transparência sobre como esses dados são utilizados e compartilhados pode ter consequências devastadoras. O indivíduo pode enfrentar violações de sua privacidade e manipulação de comportamento (como no caso de microdirecionamento para fins políticos). Por isso, é inadmissível que tais plataformas operem em um vácuo de responsabilidade.

É, portanto, imperativo reconhecer e internalizar o dever moral e ético que essas plataformas possuem. Afinal, para além da legislação, trata-se de um compromisso com a dignidade e os direitos fundamentais de seus usuários.

Diante desse cenário, algumas diretrizes podem ser formuladas com vistas à melhoria do marco normativo brasileiro no tocante à autodeterminação informativa, inclusive porque, ainda que o titular forneça seu consentimento para utilização de seus dados, tal manifestação pode ser insuficiente para garantir seu direito, conforme relatam Silva e Ehrhardt Júnior (2023), dada a assimetria de poderes, limitações cognitivas, necessidade de usufruto de serviços essenciais, emprego de termos técnicos pouco acessíveis, escassez de tempo para a leitura de longos termos contratuais e a dificuldade de prever riscos futuros decorrentes do tratamento de dados pessoais.

Em primeiro lugar, impõe-se a adoção obrigatória de políticas institucionais de proteção de dados baseadas nos princípios de *privacy by design* e *privacy by default,* previstos no artigo 25 do GDPR (União Europeia, 2016).

O princípio *privacy by design*, concebido originalmente no Canadá, consiste em defender a necessidade de garantir a privacidade de forma proativa e preventiva nas arquiteturas tecnológicas, políticas e práticas organizacionais, de modo que a proteção de dados não seja um complemento posterior, mas um elemento essencial e estruturante de todo o sistema (Cavoukian, 2010). Em vez de reagir a violações de privacidade, o modelo propõe antecipá-las e evitá-las desde o início, por meio da incorporação de salvaguardas técnicas e organizacionais. Isso inclui a adoção de medidas como a minimização de dados, a pseudonimização e a criptografia, que devem ser incorporadas de forma sistemática e não como acréscimos posteriores.

Já o princípio *privacy by default* assegura que, nas configurações padrão dos produtos e serviços, apenas os dados estritamente necessários para uma finalidade específica sejam coletados e processados, reduzindo assim a exposição desnecessária dos usuários.

Tanto o *privacy by design* como o *privacy by default* funcionam como instrumentos concretos para limitar o poder discricionário das grandes plataformas digitais, estabelecendo parâmetros objetivos de conformidade que antecedem a ocorrência de violações.

No Brasil, a LGPD (Brasil, 2018) não adotou de forma expressa os termos *privacy by design* e *privacy by default*, mas seus fundamentos estão presentes de modo implícito e principiológico na sua arquitetura normativa. Essa incorporação indireta talvez reflita uma opção do legislador brasileiro por um modelo regulatório mais flexível

A LGPD opta por uma linguagem mais aberta, que atribui à Autoridade Nacional de Proteção de Dados (ANPD), e consequentemente ao desenvolvimento jurisprudencial, a tarefa de densificar esses princípios.

É possível, contudo, identificar, na LGPD, dispositivos que traduzem materialmente os princípios *privacy by design* e *privacy by default*. O princípio da prevenção (Brasil, 2018, art. 6, inc. VIII) impõe aos agentes de tratamento o dever de adotar medidas proativas para evitar a ocorrência de danos, o que pressupõe a incorporação de salvaguardas desde a concepção de produtos e serviços. O princípio da minimização de dados (Brasil, 2018, art. 6, inc. III), por sua vez, alinha-se à lógica do *privacy by default*, ao exigir que apenas os dados estritamente necessários à finalidade pretendida sejam coletados e tratados. Além disso, o art. 46 impõe a adoção de medidas técnicas e administrativas para proteger os dados pessoais, abrindo margem para a incorporação de tecnologias voltadas à proteção da privacidade desde o início do ciclo de vida da informação.

Mostra-se também imprescindível a criação de mecanismos administrativos e judiciais céleres e acessíveis para a resolução de controvérsias relativas ao tratamento de dados pessoais, à semelhança da experiência da União Europeia, onde a autodeterminação informativa pode ser invocada como fundamento para responsabilizar controladores de dados por usos abusivos ou não consentidos de informações pessoais. Acerca do tema, o artigo

82 do GDPR (União Europeia, 2016) estabelece que qualquer pessoa que sofra dano, material ou imaterial, em razão do tratamento ilícito de dados pessoais, tem direito a ser indenizada pelo controlador ou operador responsável.

A norma adota uma lógica objetiva, impondo ao controlador o dever de reparar o dano salvo prova de que não teve qualquer responsabilidade pelo evento lesivo. Além disso, consagra a responsabilidade solidária entre os agentes de tratamento quando ambos concorrem para o mesmo fato danoso, assegurando à vítima uma compensação integral e o posterior direito de regresso entre os coobrigados.

Essa estrutura normativa reforça a centralidade da autodeterminação informativa como direito fundamental, cuja proteção exige remédios eficazes diante de práticas abusivas e desproporcionais no uso de dados pessoais. No Brasil, embora a LGPD não detalhe com a mesma qualidade técnica os mecanismos de responsabilização solidária, o seu artigo 42 admite a responsabilização dos agentes de tratamento e autoriza a reparação por danos morais e materiais, constituindo, assim, uma base normativa apta a amparar ações indenizatórias fundadas na violação da autodeterminação informativa, apesar de ter deixado de prever um sistema de responsabilidade objetiva. Ou seja, "a mera violação da legislação de proteção de dados não gera, automaticamente, o dever de reparar. Faz-se necessário que se comprove a existência de lesão a interesse existencial juridicamente tutelado." (Dantas Bisneto, 2020, p. 24). Entretanto, "ainda que o regime seja o de responsabilidade civil subjetiva, a culpa e autoria do agente de tratamento de dados são presumidas e, adicionalmente, pode haver a inversão do ônus da prova quanto aos demais pressupostos da responsabilidade civil" (Bioni; Dias, 2020, p. 19).

A jurisprudência também deve evoluir, no sentido, por exemplo, de reconhecer a existência de dano moral presumido em casos de violação à autodeterminação informativa, especialmente quando associados a práticas de vigilância invisível, microdirecionamento publicitário ou exclusão algorítmica, problemáticas ainda pouco exploradas doutrinária e jurisprudencialmente, mas que já começam a ser parte do cotidiano das pessoas.

Dessa análise, constata-se que o arcabouço de proteção do direito à autodeterminação informativa encontra-se ainda em processo de construção no Estado brasileiro. Experiências como da Alemanha e da União Europeia podem servir de referência para o aprimoramento da estrutura normativa e da prestação jurisdicional, de modo a conferir plena efetividade à autodeterminação informativa que, na era digital, tem adquirido inquestionável protagonismo.

4 Considerações finais

Os direitos fundamentais, especialmente o direito à autodeterminação informativa, enfrentam desafios sem precedentes na era digital. O artigo procurou demonstrar que, à medida que as plataformas digitais se tornam onipresentes em nossas vidas, coletando e monetizando dados pessoais em larga escala, a privacidade e a autodeterminação informativa dos usuários estão cada vez mais em risco. Essa dinâmica coloca em questão o quadro normativo existente e demanda uma reavaliação crítica da aplicabilidade dos direitos fundamentais em contextos digitais.

Os objetivos delineados no artigo foram atendidos, à medida que se evidenciou como o direito à autodeterminação informativa é impactado nas interações digitais, além de formular diretrizes para aprimorar sua proteção.

Conclui-se que é imperativo um esforço conjunto de governos, empresas, organizações da sociedade civil e indivíduos para desenvolver políticas, regulamentações e práticas tecnológicas que assegurem autonomia do indivíduo sobre seus dados pessoais, promovendo assim uma sociedade digital mais justa, inclusiva e democrática.

Nesse sentido, foram apresentadas algumas experiências jurisprudenciais forâneas, como decisões do Tribunal Constitucional Federal Alemão e do Tribunal de Justiça da União Europeia, bem como experiências normativas, a exemplo do Regulamento Geral sobre a Proteção de Dados (União Europeia, 2016) que incorporou os princípios de *privacy by design* e *privacy by default* no GDPR (União Europeia, 2016). Recorreu-se também ao GDPR para apresentar alguns mecanismos céleres e acessíveis para a resolução de controvérsias relativas ao tratamento de dados pessoais, especialmente no que se refere à responsabilização solidária dos controladores e operadores.

O desafio reside em garantir que os avanços tecnológicos contribuam positivamente para a humanidade, sem comprometer os direitos fundamentais. Reconhecer e reforçar a proteção desses direitos torna-se, portanto, um imperativo ético-jurídico na construção de uma ordem global que respeite a dignidade de cada pessoa humana no mundo digital.

Referências

ALEMANHA. **Urteil vom 1. Oktober 2024, 1 BvR 1160/19.** Leitsätze zum Urteil des Ersten Senats vom 1. Oktober 2024. Karlsruhe: Bundesverfassungsgericht, 2024. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2024/10/rs20241001_1bvr116019.html Acesso em: 14 jun. 2025.

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, B.; DIAS, D. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica**, Rio de Janeiro, v. 9, n. 3, p. 1-23, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662. Acesso em: 18 jun. 2025.

BOBBIO, N. **A era dos direitos**. Rio de Janeiro: Elsevier, 2004.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 maio. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados – LGPD. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 10 maio. 2024

BRASIL. **Ação direta de inconstitucionalidade nº 6387, de 07 de maio de 2020.** Referendo na medida cautelar na ação direta de inconstitucionalidade 6.387 Distrito Federal. Brasília, DF: Supremo Tribunal Federal, 2020. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 10 maio. 2024.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Câmara dos Deputados; Senado Federal, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 10 maio. 2024.

BRASIL. **Medida provisória nº 954, de 17 de abril de 2020.** Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 10 maio. 2024.

CANOTILHO, J. J. G. Sobre a indispensabilidade de uma Carta de Direitos Fundamentais Digitais da União Europeia. **Revista do Tribunal Regional Federal da Primeira Região**, Brasília, v. 31, n. 1, p. 69–75, 2019. Disponível em: https://revista.trf1.jus.br/trf1/article/view/17. Acesso em: 04 jun. 2025.

CANTARINI, P. Desafios ao estado democrático de direito - inteligência artificial, direitos fundamentais e constitucionalismo digital. **Revista Jurídica Unicuritiba**, Curitiba, v. 2, n. 74, p. 800–836, 2023. Disponível em: https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/6888/pdf. Acesso em: 05 jun. 2025.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz & Terra, 2000.

CAVOUKIAN, A. Privacy by design: the 7 foundational principles. Implemation and mapping of fair information practices. **Information Society**, [*s. l.*], v. 3, n. 2, p. 261–267, 2010. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf Acesso em: 14 jun. 2025.

CELESTE, E. Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital. **Direitos Fundamentais & Justiça**, Porto Alegre, v. 15, n. 45, p. 63-91, 2021. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1219/1043 Acesso em: 24 jun. 2025.

DANTAS BISNETO, C. Reparação por danos morais pela violação à LGPD e ao RGPD: uma abordagem de direito comparado. **Civilística**, Rio de Janeiro, v. 9, n. 3, p. 1-29, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/493. Acesso em: 18 jun. 2025.

DONEDA, D. C. M. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. *In:* TEPEDINO, G. (coord.). **Problemas de direito civil-constitucional**. Rio de Janeiro: Renovar, 2000. p. 111-136.

GSTREIN, O. J.; BEAULIEU, A. How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. **Philosophy & Technology**, [*s. l.*], v. 35, n. 3, p. 1-38, 2022. Disponível em: https://link.springer.com/article/10.1007/s13347-022-00497-4. Acesso em: 14 jun. 2025.

LIMBERGER, T. Da evolução do direito a ser deixado em paz à proteção dos dados pessoais. **Revista Novos Estudos Jurídicos**, Vale do Itajaí, v. 14, n. 2, p. 27-53, 2009. DOI: https://doi.org/10.17058/rdunisc.v0i30.580

MENDES, L. S. F. Autodeterminação informativa: a história de um conceito. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 25, n. 4, p. 1–18, out./dez. 2020. Disponível em: https://ojs.unifor.br/rpen/article/view/10828/pdf. Acesso: 24 jun. 2025.

MORAES, A. de. **Direitos humanos fundamentais**: teoria geral. 2. ed. São Paulo: Atlas, 1998.

PARDO, D. W. de A. **Direitos fundamentais não enumerados**: justificação e aplicação. 2015. Tese (Doutorado em Direito) – Centro de Ciências Jurídicas, Universidade Federal de Santa Catarina, Florianópolis, 2015. Disponível em: https://repositorio.ufsc.br/handle/123456789/102251. Acesso em: 24 jun. 2025.

PESSOA, J. P. S.; LIMBERGER, T.; WITSCHORECK, P. V. dos S. O direito à proteção de dados pessoais na fronteira do capitalismo de dados e do colonialismo digital. **Pensar – Revista de Ciências Jurídicas**, Fortaleza, v. 29, n. 4, p. 1-13, out./dez. 2024. DOI: https://doi.org/10.5020/2317-2150.2025.15201

PIOVESAN, F. **Temas de direitos humanos**. São Paulo: Max Limonad, 1998.

RODOTÀ, S. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SARLET, I. W. Proteção de dados como direito fundamental na Constituição Federal Brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Porto Alegre, v. 14, n. 42, p. 179-218, jan./jun. 2020. DOI: https://doi.org/10.30899/dfj.v14i42.875

SILVA, G. B. P; EHRHARDT JÚNIOR, M. Challenges to enforcing informative self-determination under the general law of data protection (GLDP). **Civilistica**, Rio de Janeiro, v. 12, n. 1, p. 1-16, 2023.

SOUZA, J. F. V. de; MEZZAROBA, O. Direitos humanos no século XXI: uma utopia possível ou uma quimera irrealizável? *In:* BAEZ, L. N. X.; SILVA, R. N. da; SMORTO, G. (org.). **Os desafios dos direitos fundamentais na América Latina e na Europa.** Joaçaba: Editora Unoesc, 2012. p. 175-176.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Processo C-131/12, de 13 de maio de 2014.** Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. Luxemburgo: TJUE, 2014. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131. Acesso em: 14 jun. 2025.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão C-311/18 - Facebook Ireland e Schrems, de 16 de julho de 2020.** Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais. Irlanda: TJUE, 2020. Disponível em: https://curia.europa.eu/juris/liste.jsf?num=C-311/18 Acesso em: 14 jun. 2025.

UNIÃO EUROPEIA. Carta dos direitos fundamentais da União Europeia. **Jornal Oficial da União Europeia**, Luxemburgo, 26 out. 2012. Disponível em: https://eur-lex.europa.eu/eli/treaty/char_2012/oj. Acesso em: 02 jun. 2025.

UNIÃO EUROPEIA. **Regulamento 679, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados – GDPR). Bruxelas: UE, 2016. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679 . Acesso em: 02 jun. 2025.

ZUBOFF, S. What is surveillance capitalism? **New Labor Forum**, [*s. l.*], v. 28, n. 1, p. 10-29, 2019. Disponível em: https://www.oru.se/contentassets/911b03b7ff614b14a58782b9ee183bf2/zuboff-2019.pdf . Acesso em: 03 jun. 2025.